# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-342270
(43)Date of publication of application : 29.11.2002

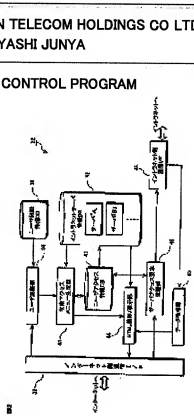
(51)Int.Cl. G06F 15/00
G06F 12/00
G06F 12/14
G06F 13/00

(21)Application number : 2001-145886
(22)Date of filing : 16.05.2001

(71)Applicant : JAPAN TELECOM HOLDINGS CO LTD
(72)Inventor : KOBAYASHI JUNYA

## (54) REMOTE ACCESS CONTROL METHOD AND REMOTE ACCESS CONTROL PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To perform an access from the outside to a server on an intranet without having to conduct complicated input on the part of a user.
SOLUTION: A remote access control server 22 is provided with a user authenticating part 34 for receiving log-in and user ID and a password from a portable terminal 14, and for authenticating the user, an initial access menu generating part 38 for generating a list related with a server which can be accessed by the authenticated user, and for transmitting the list to a portable terminal 14, an access information receiving part 46 for specifying the server to be accessed on the intranet 24, based on an item selected from the list, and for acquiring authentication information specific to the user related with the server, and for transmitting the authentication information through the intranet 24, and for realizing the transmission of contents, in response to the user authentication and the selected item, and an information acquiring part 50 for receiving the contents, in response to the item from the server. Then, the acquired contents are transmitted to the portable terminal 14.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－342270
（P2002－342270A）
(43)公開日　平成14年11月29日(2002.11.29)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　15/00 | ３１０ | Ｇ０６Ｆ　15/00 | ３１０Ｄ | ５Ｂ０１７ |
| | ３３０ | | ３３０Ｂ | ５Ｂ０８２ |
| 12/00 | ５３７ | 12/00 | ５３７Ｄ | ５Ｂ０８５ |
| | ５４６ | | ５４６Ａ | |
| 12/14 | ３２０ | 12/14 | ３２０Ｃ | |

審査請求　未請求　請求項の数10　ＯＬ　（全 11 頁）　最終頁に続く

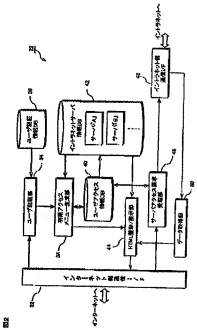
(21)出願番号　特願2001－145886(P2001－145886)
(22)出願日　平成13年５月16日(2001.5.16)

(71)出願人　000229265
日本テレコムホールディングス株式会社
東京都中央区八丁堀四丁目７番１号
(72)発明者　小林　鋪也
東京都中央区八丁堀四丁目７番１号　日本テレコム株式会社内
(74)代理人　100103832
弁理士　益田　英一郎　（外１名）

Ｆターム（参考）　5B017 AA07 BA05 CA16
5B082 GA11 HA08
5B085 AE01 AE23 BC07

(54)【発明の名称】　リモートアクセス制御方法、リモートアクセス制御プログラム

(57)【要約】
【課題】　ユーザによる煩雑な入力なしに、イントラネット上のサーバに外部からアクセスする。
【解決手段】　リモートアクセス制御サーバ２２は、携帯端末１４からログインおよびユーザＩＤおよびパスワードを受理して、ユーザを認証するユーザ認証部３４と、認証されたユーザがアクセス可能なサーバに関するリストを生成して、当該リストを、携帯端末１４に伝達する初期アクセスメニュー生成部３８と、携帯端末１４からの、リストから選択された項目に基づき、イントラネット２４上のアクセスすべきサーバを特定して、サーバに関するユーザ固有の認証情報を取得して、イントラネット２４を介して認証情報を伝達して、ユーザ認証および選択された項目に応答したコンテンツの伝達を求めるアクセス情報受理部４６と、サーバから、項目に応答したコンテンツを受理する情報取得部５０とを備え、取得したコンテンツが携帯端末１４に伝達されるようになっている。



【特許請求の範囲】

【請求項１】　所定のネットワークに接続された複数のサーバに、当該ネットワークの外部の端末からアクセスするためのリモートアクセス制御方法であって、

前記所定のネットワークに接続されたリモートアクセス制御サーバにおいて、

前記端末によるアクセスをなすユーザによる前記ネットワークへのログインのための認証情報を登録するステップと、

前記ユーザがアクセス可能な前記ネットワーク上のサーバのそれぞれに関する、当該ユーザの固有の認証情報を登録するステップと、

前記端末からの、前記ログインのための認証情報の受理に応答して、ユーザを認証するステップと、

認証されたユーザがアクセス可能なサーバに関するリストを生成して、当該リストを、前記端末に伝達するステップと、

前記端末からの、リストから選択された項目に基づき、前記ネットワーク上のアクセスすべきサーバを特定するステップと、

前記サーバに関する前記ユーザの固有の認証情報を取得して、当該サーバに対して、認証情報を伝達して、ユーザ認証および選択された項目に応答したコンテンツの伝達を求めるステップと、

前記サーバから、前記項目に応答したコンテンツを受理するステップと、

受理したコンテンツを、前記端末に伝達するステップとを備えたことを特徴とするリモートアクセス制御方法。

【請求項２】　前記ユーザの固有の認証情報を登録するステップが、前記認証の種別を含み、

前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、前記認証の種別にしたがった情報の伝達を行うことを特徴とする請求項１に記載のリモートアクセス制御方法。

【請求項３】　前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、ベーシック認証におけるユーザＩＤおよびパスワードを伝達するステップを含むことを特徴とする請求項１または２に記載のリモートアクセス制御方法。

【請求項４】　さらに、前記受理したコンテンツにリンクが含まれる場合に、前記リンクを、前記リモートアクセスサーバを介した形態のものに変換するステップを備えたことを特徴とする請求項１ないし３の何れか一項に記載のリモートアクセス制御方法。

【請求項５】　さらに、前記コンテンツにおけるフォントサイズの変更、テーブルの列幅の調整を含むコンテンツ表示形態の調整、および／または、不要なタグの消去を含む、コンテンツを整形するステップを備えたことを特徴とする請求項１ないし４の何れか一項に記載のリモートアクセス制御方法。

【請求項６】　所定のネットワークに接続された複数のサーバへの、当該ネットワークの外部の端末からアクセスを制御するプログラムを、前記外部と前記所定のネットワークとの間に介在したサーバに実行させるリモートアクセス制御プログラムであって、

前記所定のネットワークに接続されたリモートアクセス制御サーバにおいて、

前記端末によるアクセスをなすユーザによる前記ネットワークへのログインのための認証情報を登録するステップと、

前記ユーザがアクセス可能な前記ネットワーク上のサーバのそれぞれに関する、当該ユーザの固有の認証情報を登録するステップと、

前記端末からの、前記ログインのための認証情報の受理に応答して、ユーザを認証するステップと、

認証されたユーザがアクセス可能なサーバに関するリストを生成して、当該リストを、前記端末に伝達するステップと、

前記端末からの、リストから選択された項目に基づき、前記ネットワーク上のアクセスすべきサーバを特定するステップと、

前記サーバに関する前記ユーザの固有の認証情報を取得して、当該サーバに対して、認証情報を伝達して、ユーザ認証および選択された項目に応答したコンテンツの伝達を求めるステップと、

前記サーバから、前記項目に応答したコンテンツを受理するステップと、

受理したコンテンツを、前記端末に伝達するステップとを、前記制御サーバに実行させることを特徴とするリモートアクセス制御プログラム。

【請求項７】　前記ユーザの固有の認証情報を登録するステップが、前記認証の種別を含み、

前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、前記認証の種別にしたがった情報の伝達を行うように、前記制御サーバを動作させることを特徴とする請求項６に記載のリモートアクセス制御プログラム。

【請求項８】　前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、ベーシック認証におけるユーザＩＤおよびパスワードを伝達するステップを含むように、前記制御サーバを動作させることを特徴とする請求項６または７に記載のリモートアクセス制御プログラム。

【請求項９】　さらに、前記受理したコンテンツにリンクが含まれる場合に、前記リンクを、前記リモートアクセスサーバを介した形態のものに変換するステップを、前記制御サーバに実行させることを特徴とする請求項６ないし８の何れか一項に記載のリモートアクセス制御プログラム。

【請求項１０】　さらに、前記コンテンツにおけるフォ

ントサイズの変更、テーブルの列幅の調整を含むコンテンツ表示形態の調整、および/または、不要なタグの消去を含む、コンテンツを整形するステップを、前記制御サーバに実行させることを特徴とする請求項６ないし９の何れか一項に記載のリモートアクセス制御プログラム。

【発明の詳細な説明】

【０００１】

【産業上の技術分野】本発明は、複数のサーバを有する一定のネットワーク、たとえば、社内イントラネットにアクセスする手法に関する。

【０００２】

【従来の技術】企業、地方公共団体などの組織内においては、サーバと多数の端末とを有線或いは無線にて接続して、情報を共有化するネットワークであるイントラネットが普及している。ここでは、ユーザは、端末から自己のアクセスが認められているサーバにアクセスして、必要な情報を引き出し、或いは、必要な情報を書き込むことができるようになっている。

【０００３】上記組織の構成員、たとえば、企業の社員などが、イントラネットの外部から、当該イントラネット上のサーバにアクセスして、必要な情報を取得する必要性がある。これは、イントラネット上の一端を、所定の機器（たとえば、ゲートウェイ、ルータ）などを介して、インターネットに接続し、外部のコンピュータからインターネットを経て、イントラネット上のサーバ等にアクセス可能とすることにより実現される。特に、近年、パーソナルコンピュータによるアクセスではなく、インターネットに接続可能な携帯電話、ＰＤＡなどの携帯端末によるアクセス可能とすることが望まれる。

【０００４】

【発明が解決しようとする課題】上記イントラネット上のサーバ等にアクセスする場合に、ユーザは、基本的には、自己が当該サーバをアクセスするためのパスワードなどの認証情報を、サーバに与える必要がある。たとえば、ベーシック認証においては、サーバごとに、自分のユーザＩＤおよびパスワードを入力し、サーバにおける認証の後、サーバとのアクセスが認められる。したがって、イントラネット上のサーバが複数存在する場合に、サーバごとの認証が必要となり、ユーザは、アクセスに至るまでに幾度となく認証情報の入力をする必要がある。また、サーバごとの認証では、各サーバ内のコンテンツ制御も煩雑となる。

【０００５】本発明は、ユーザによる煩雑な入力なしに、一定のサーバにアクセス可能となるような手法を提供することを目的とする。

【０００６】

【課題を解決するための手段】本発明の目的は、所定のネットワークに接続された複数のサーバに、当該ネットワークの外部の端末からアクセスするためのリモートアクセス制御方法であって、前記所定のネットワークに接続されたリモートアクセス制御サーバにおいて、前記端末によるアクセスをなすユーザによる前記ネットワークへのログインのための認証情報を登録するステップと、前記ユーザがアクセス可能な前記ネットワーク上のサーバのそれぞれに関する、当該ユーザの固有の認証情報を登録するステップと、前記端末からの、前記ログインのための認証情報の受理に応答して、ユーザを認証するステップと、認証されたユーザがアクセス可能なサーバに関するリストを生成して、当該リストを、前記端末に伝達するステップと、前記端末からの、リストから選択された項目に基づき、前記ネットワーク上のアクセスすべきサーバを特定するステップと、前記サーバに関する前記ユーザの固有の認証情報を取得して、当該サーバに対して、認証情報を伝達して、ユーザ認証および選択された項目に応答したコンテンツの伝達を求めるステップと、前記サーバから、前記項目に応答したコンテンツを受理するステップと、受理したコンテンツを、前記端末に伝達するステップとを備えたことを特徴とするリモートアクセス制御方法により達成される。

【０００７】本発明によれば、制御サーバにおいて、所定のネットワーク、たとえば、社内イントラネットに接続された複数のサーバのそれぞれについて、ユーザがアクセス可能なサーバ、および、各サーバのユーザ固有の認証情報が登録されている。ユーザによる外部からの、所定のネットワークへのログイン要求に応答して、ユーザがアクセス可能な、当該ネットワーク上のサーバが見出され、これに関するリストがユーザの端末に提示される。ユーザのリスト中の項目の選択、すなわち、あるサーバへのアクセス要求に応答して、アクセス先のサーバに関するユーザ固有の認証情報が、登録された情報から取り出され、これを利用して、ユーザによる直接の認証の代理として、制御サーバによりネットワーク上のサーバに認証が依頼される。したがって、ユーザは、当該所定のネットワーク上のサーバにアクセスするたびに、認証のための入力、たとえば、ユーザＩＤやパスワードの入力の必要なく、自己がアクセスを認められている所望のサーバへのアクセスをなすことが可能となる。

【０００８】本発明の好ましい実施態様においては、前記ユーザの固有の認証情報を登録するステップが、前記認証の種別をも含み、前記サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝送するステップが、前記認証の種別にしたがった情報の伝達を行うように構成されている。これにより、ＨＴＴＰサーバ、メールサーバなど多種多様なサーバに対して、制御サーバが代理認証をなすことが可能となる。

【０００９】より好ましい実施態様においては、サーバに関する前記ユーザ固有の認証情報を、前記サーバに対して伝達するステップが、ベーシック認証におけるユーザＩＤおよびパスワードを伝達するステップを含む。

【００１０】別の好ましい実施態様においては、さらに、前記受理したコンテンツにリンクが含まれる場合に、前記リンクを、前記リモートアクセスサーバを介した形態のものに変換するステップを備えている。

【００１１】さらに、前記コンテンツにおけるフォントサイズの変更、テーブルの列幅の調整を含むコンテンツ表示形態の調整、およびノまたは、不要なタグの消去を含む、コンテンツを整形するステップを備えているのがより望ましい。携帯電話などディスプレイの小さな端末にコンテンツを伝達する場合に、これは特に有効である。

【００１２】また、本発明の目的は、上記ステップを、制御サーバに実行させるためのリモートアクセス制御プログラムによっても達成される。

【００１３】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態につき説明を加える。図１は、本発明の実施の形態にかかるデータ通信システムの概略を示す図である。図１に示すように、本実施の形態にかかるデータ通信システムは、インターネット１２に、携帯電話やＰＤＡなどの携帯端末１４－１、・・・、１４－ｎが接続されている。以下、単一の携帯端末を説明する際に、単に、「携帯端末１４」と称する。

【００１４】また、インターネット１２には、携帯端末１４がインターネット２４に接続されたサーバ２６－１、・・・、２６－ｍにアクセスする際に必要な処理を実行する制御システム１６が接続されている。サーバに関しても、携帯端末１４からのアクセスにかかるサーバを、単に、「サーバ２６」と称する。

【００１５】制御システム１６は、携帯端末１４との間でのインターネット１２を介した通信の際に、データを、たとえば、ＳＳＬに基づき暗号化し、或いは、暗号化されたデータを復号化するリバースプロキシサーバ１８と、ＨＴＭＬのコンテンツを、携帯端末用の、言語のコンテンツに翻訳するＨＴＭＬ変換サーバ（トランスコードサーバ）２０と、インターネット２４へのアクセスの際に、後述する認証の代理などの処理を実行するリモートアクセス制御サーバ２２とを有している。制御システム１６のリモートアクセス制御サーバ２２は、インターネット２４に接続されている。このインターネット２４には、種々のサーバ２６－１、・・・、２６－ｍが接続されている。

【００１６】このシステムにおいては、インターネット１２の間と、インターネット２４との間は、制御システム１６にて隔てられている。たとえば、制御システム１６には、ファイアウォールが形成され、オーソライズされていないユーザによる、インターネット１２の側からのインターネット２４を介したアクセスが出来ないようになっている。たとえば、企業内のサーバ２６－１、・・・、２６－ｍを、インターネット２４にて接続した形態を考える。企業内においては、社員つまりユーザが、クライアントマシンを操作してインターネット２４にログインして、当該インターネット２４上の、ユーザがアクセス可能なサーバにアクセスして、必要な情報を取得する。その一方、社外からのアクセスの際には、携帯端末１４を利用して、制御システム１６を介して、インターネット２４にログインして、インターネット２４上のサーバ２６にアクセスすることになる。

【００１７】次に、本実施の形態にかかるリモートアクセス制御サーバ２２につき説明を加える。なお、リバースプロキシサーバ１８およびＨＴＭＬ変換サーバ（トランスコードサーバ）２０は、現段階で公知であるため、その機能の説明を省略する。図２は、本実施の形態にかかるリモートアクセス制御サーバ２２の構成を示すブロックダイヤグラムである。図２に示すように、リモートアクセス制御サーバ２２は、インターネット１２の側に接続され、当該インターネット１２側との通信を制御するインターネット側通信Ｉ／Ｆ３２を備えている。実際には、インターネット側通信Ｉ／Ｆ３２は、ＨＴＭＬ変換サーバ２０に接続され、携帯端末１４からの情報を受理し、或いは、携帯端末１４に供給すべきデータ（コンテンツ）を伝達する。

【００１８】また、リモートアクセス制御サーバ２２は、インターネット１２を介してアクセスしたユーザのインターネット２４へのログインの際の認証を実行するユーザ認証部３４と、上記インターネット２４へのログインの際に、ユーザを認証するための情報（ユーザＩＤ（ＵＩＤ）やパスワード（ｐｗｄ））を記憶したユーザ認証情報データベース（ＤＢ）３６と、ユーザによる初期的なアクセスに応答して、必要なメニューを作成する初期アクセスメニュー生成部３８と、各ユーザがアクセス可能なサーバを示す情報が記憶されたユーザアクセス情報ＤＢ４０と、イントラネットに接続された各サーバについての種々の情報が記憶されたイントラネットサーバ情報ＤＢ４２と、携帯端末１４に与えるためにコンテンツ中のＵＲＬを変更し、また、不要なタグ等を除去する処理を実行するＨＴＭＬ整形／表示部４４と、初期的なアクセスの後、ユーザの携帯端末からのアクセス要求を受理して、必要な処理、特に、後述する代理認証の処理を実行するサーバアクセス要求受理部４６と、イントラネット２４と接続され、各サーバ２６とのデータ通信を制御するイントラネット側通信Ｉ／Ｆ４８と、イントラネット２４を介して伝達されたコンテンツ等を取得するデータ取得部５０とを有している。

【００１９】本実施の形態にかかるユーザ認証情報ＤＢ３６、ユーザアクセス情報ＤＢ４０、およびイントラネットサーバ情報ＤＢ４２には、後述するような必要な情報が、予め登録されている。たとえば、ユーザ認証情報ＤＢ３６へのユーザＩＤおよびパスワードの登録は、携帯端末１４を用いて行っても良いし、イントラネット

２４の側から（つまり、イントラネット２４上の管理サーバなどから）行っても良い。また、ユーザアクセス情報ＤＢ４０およびイントラネットサーバ情報ＤＢ４２への登録は、イントラネット２４の側から行うのが望ましい。

【００２０】このように構成されたリモートアクセス制御サーバ２２を介したデータ通信につき、以下に説明を加える。図３および図５は、携帯端末１４、リモートアクセス制御サーバ２２などにて実行される処理を示すフローチャートである。特に、図３は、携帯端末１４からの初期的なアクセスの際に実行される処理を示している。図３において、携帯端末１４とリモートアクセス制御サーバ２２との間には、リバースプロキシサーバ１８およびＨＴＭＬ変換サーバ２０が介在しているが、これらサーバ１８、２０に関しては破線にて示し、その処理内容についての説明も省略している。

【００２１】図３において、携帯端末１４からのログイン要求あり、携帯端末１４からイントラネット２４へのログイン用のユーザＩＤ（ＵＩＤ）およびパスワード（ｐｗｄ）が伝達されると（ステップ３０１）、リモートアクセス制御サーバ２２は、これを受理してユーザを認証する（ステップ３０２）。より詳細には、ユーザ認証部３４が、ユーザ認証情報ＤＢ３６に登録された、ユーザＩＤおよびそれに関連付けられたパスワードと、携帯端末１４から伝達されたものとを照合する。

【００２２】ユーザ認証が終了すると、初期アクセスメニュー生成部３８が、ユーザアクセス情報ＤＢ４０を参照して、ユーザがアクセス可能なサーバ等の情報を取得するとともに、イントラネットサーバ情報ＤＢ４２をアクセスして、ユーザがアクセス可能なサーバに関する情報を取得して、所定のメニューを生成する（ステップ３０３）。図４（ａ）は、ユーザアクセス情報ＤＢ４０中のデータ構造の例を示す図である。

【００２３】図４（ａ）に示すように、ユーザアクセス情報ＤＢ４０においては、ユーザごとにアクセス可能なサーバの名称、および、当該サーバの種別が記述されている（符号４０１、４０２参照）。たとえば、ユーザ「ａ」（ユーザＩＤ：ｕｓｅｒａ）に関しては、デフォルト、ｈｔｔｐサーバであるサーバ「Ａ」（サーバ名：ｓｅｒｖｅｒＡ）、メールサーバであるサーバ「Ｂ」（サーバ名：ｓｅｒｖｅｒＢ）、ｈｔｔｐサーバであるサーバ「Ｄ」（サーバ名：ｓｅｖｅｒＤ）などにアクセス可能となっている（符号４１１、４１２参照）。

【００２４】したがって、ユーザ「ａ」によるアクセスがあった場合には、初期アクセスメニュー生成部３８は、ユーザアクセス情報ＤＢ４０のうち、ユーザＩＤ「ｕｓｅｒａ」に関するデータ（符号４１２）を参照して、ユーザ「ａ」がアクセス可能なサーバを特定する。次いで、イントラネットサーバ情報ＤＢ４２のうち、当該ユーザがアクセス可能なサーバの各々に関するデータ領域を参照する。

【００２５】本実施の形態において、イントラネットサーバ情報ＤＢ４２においては、各ユーザに共通にアクセス可能なサーバ情報であるデフォルト情報領域と、各サーバの情報領域とが設けられている。図４（ｂ）は、デフォルト情報領域の例を示す図である。ここでは、メニューにリストされる際の優先順位（Ｐｒｉｏｒｉｔｙ）、アクセス先サーバ（Ｓｅｒｖｅｒ）、アクセス先のコンテンツのタイトル（Ｔｉｔｌｅ）、当該アクセス先のＵＲＬ（Ｕｒｌ）、携帯端末１４にコンテンツを伝達する際に、元のコンテンツから消去すべきタグの情報（Ｄｅｌｅｔｅ ＴＡＧ）、および、整形情報（Ｆｏｒｍａｔ）が含まれる。

【００２６】携帯端末１４に対して、送信するデータ量を小さくするのが望ましい。このため、本字風景の形態においては、ＩＭＧタグなどをコンテンツから削除できるようにしている。また、携帯端末１４の表示装置の画面上にコンテンツを表示するため、フォントサイズを変更し、また、テーブルの列幅を調整する必要がある。このため、整形フォーマットには、上記フォントの変更や列幅の調整に関する記述が含まれ得る。さらに、コンテンツにはリンクが含まれる場合がある。本実施の形態において、外部からは、上記リンクに直接アクセスすることはできない。したがって、ＵＲＬを変換するための情報が記述される場合もある。なお、図４（ｂ）の例において、先頭行の「ｉｓｉ」はリストスタート用プリミタ、末尾の「ｉｅｉ」はリストエンド用のプリミタである。図４（ｂ）において、優先度は「０（最優先）」、サーバ名は「サーバＡ（ｓｅｖｅｒＡ）」、タイトルは「サーバ「Ａ」の基本コンテンツ」であることなどが示される。

【００２７】また、図６は、各サーバの情報領域の例を示す図である。図６に示すように、情報領域６００には、サーバ「Ａ（ｓｅｖｅｒＡ）に関する情報領域（符号６０１参照）、サーバ「Ｂ」（ｓｅｖｅｒＢ）に関する情報領域（符号６０２参照）、サーバ「Ｃ」（ｓｅｖｅｒＣ）に関する情報領域（符号６０３参照）などが含まれる。

【００２８】本実施の形態において、各情報領域には、当該サーバにアクセス可能なユーザごとに、以下に述べる項目を示す値が収容されている。サーバがウェブサーバである場合には、情報領域６０１には、アクセス可能なユーザ（たとえば、ユーザＩＤが「ｕｓｅｒａ」）に関して、メニューにリストされる際の優先順位（Ｐｒｉｏｒｉｔｙ）、ベーシック認証をすべきか否かを示すフラグ（Ｂａｓｉｃ Ａｕｔｈ）、ベーシック認証時の保護領域（Ｒｅａｌｍ）などが含まれる。サーバがメールサーバである場合には、情報領域６０２には、当該ユーザがメールサーバをアクセスする際の固有のパスワード（Ｐａｓｓｗｏｒｄ）などが含まれる。なお、情報領域

６０１、６０２、・・・には、サーバをアクセス可能なユーザごとに必要な項目の値が取得されるため、各ユーザに関する項目の値の最終行には、エンドオブユーザデリミタ（ｅｕｃ）が記述されている。

【００２９】フラグ「ＢａｓｉｃＡｕｔｈ」は、サーバによる認証がベーシック認証であるか否かを示している。また、保護領域「Ｒｅａｌｍ」は、ベーシック認証によるパスワードにて保護される領域を示す。「Ｒｅａｌｍ＝／ｔｅｓｔ」であった場合には、「／ｔｅｓｔ」以降の全ての領域、たとえば、

「http://serveraddress/test/index.html」

「http://severaddress/test/subfolder/index.html」

などへのアクセスに際して、パスワードが必要であることを示している。初期アクセスメニュー生成部３８は、アクセスにかかるユーザに関して、当該ユーザがアクセス可能なサーバの情報領域から、当該ユーザに関する項目の値を取得する。

【００３０】次いで、アクセス可能なサーバ（より詳細には、サーバのＵＲＬ）を示すタイトルからなるメニューを生成する。必要な場合には、フォントの変更、タグの削除などを含むメニューの整形などの処理を、ＨＴＭＬ整形／表示部４４が実行する。このようにして作られたメニュー画像は、ＨＴＭＬ変換サーバ２０およびリバースプロキシサーバ１８を介して、インターネット１２に送出され、アクセス元である携帯端末１４に伝達される（ステップ３０５）。携帯端末１４の表示装置の画面上には、アクセス可能なコンテンツのタイトルが列挙されたメニュー画像が表示される（ステップ３０６）。

【００３１】次に、メニュー画像から所定のメニュー項目を選択した後に実行される処理につき、図５を参照して説明する。なお、図５において、携帯端末１４とリモートアクセス制御サーバ２２との間に介在するリバースプロキシサーバ１８およびＨＴＭＬ変換サーバ２０は省略している。

【００３２】ユーザが携帯端末１４のキーを操作して、所定のメニュー項目を選択すると、サーバアクセス要求受理部４６が、このアクセス要求を受理する。ここで、図３のステップ３０５にて返信した情報には、セッションＩＤが含まれている。したがって、ステップ５０１におけるアクセス要求を受理したサーバアクセス要求受理部４６は、セッションＩＤに基づいてユーザを特定する。次いで、サーバアクセス要求受理部４６は、ユーザのアクセス要求にかかるサーバを特定して、イントラネットサーバ（情報ＤＢ４２から、当該サーバに関する情報領域中、アクセスしたユーザの固有パスワードを取得する（ステップ５０２、５０３）。

【００３３】その後に、ベーシック認証の代理処理（ステップ５０４）が実行される。より詳細には、ユーザがアクセス要求したＵＲＬに、イントラネット２４を介して、アクセスして（ステップ５０５）、そこで、ユーザＩＤ（ＵＩＤ）と、イントラネットサーバ情報ＤＢ４２から取得した、当該サーバアクセスにかかるユーザ固有のパスワード（ｐｗｄ）をアクセス先（たとえば、サーバ「Ａ」）に伝達する（ステップ５０６）。アクセス先のサーバにおいては、当該ユーザＩＤおよび固有のパスワードに基づきユーザを認証し、正当なユーザである場合には、所定のコンテンツを、イントラネット２４を介してリモートアクセス制御サーバ２２に伝達する（ステップ５０８）。

【００３４】リモートアクセス制御サーバ２２は、取得したデータ（コンテンツ）が、ＨＴＭＬでない場合（たとえば、アクセス先が、ウェブサーバではなく、メールサーバやデータベースサーバであった場合）には、取得したデータに基づくＨＴＭＬデータを生成する（ステップ５０９）。次いで、リモートアクセス制御サーバ２２は、サーバに関する情報領域から不要タグや整形フォーマットに関する情報に基づき、データを整形する（ステップ５１０）。このようにして作られたデータ（コンテンツ）が、携帯端末１４に伝達される（ステップ５１１）。このようにして、携帯端末１４の表示装置の画面上には、ユーザが選択したメニュー項目に応答したコンテンツが表示される（ステップ５１２）。

【００３５】図７は、上記図３および図５にて示す処理により携帯端末１４の表示装置の画面上に表示された画像の例を示す図である。ユーザによりログインの際には、携帯端末１４の表示装置の画面上には、図７（ａ）に示す画像７０１が表示される。ユーザは、携帯端末１４のキーを操作して、入力欄７０２、７０３に、それぞれ、ユーザＩＤおよびパスワードを記入する。このユーザＩＤおよびパスワードは、リモートアクセス制御サーバ２２に登録されたものを利用すればよい。図７（ｂ）は、これに応答して、ステップ３０５において伝達されたメニュー画像の例を示している。メニュー画像７１１から所定のメニュー項目（たとえば、「事務連絡掲示板（符号７１２参照）」）を選択すると、図５に示す処理が実行される。

【００３６】再度説明すると、「事務連絡掲示板」へのアクセス要求（ステップ５０１）に応答して、当該「事務連絡掲示板」に関するサーバの情報領域から、アクセスしたユーザの固有パスワードが取り出され、イントラネット２４を介して、上記サーバに対して、ユーザＩＤおよび取り出された固有パスワードが伝達される（ステップ５０６）。サーバにおいては、認証（ステップ５０７）の後、所定のコンテンツがリモートアクセス制御サーバ２２に伝達される（ステップ５０８）。リモートアクセス制御サーバ２２は、所定の処理（ステップ５０９、５１０）の後、コンテンツを携帯端末１４に、インターネット１２を介して伝達する（ステップ５１１）。図７（ｃ）は、このようにして携帯端末１４の表示装置の画面上に表示された画像７２１を示す。ここで、ユー

ザは、メニューから所望の項目を選択した後、当該メニュー項目に関するサーバのアクセスの際に、パスワードの入力などを行う必要がない。したがって、余分なキー入力なしに、自己がアクセスを認められている、イントラネット２４上の所望のサーバにアクセスすることが可能である。

【００３７】上記図５を参照した処理は、イントラネット２４上のウェブサーバへのアクセスに関していたが、他のサーバ（たとえば、メールサーバやデータベースサーバ）に関連しても、代理認証の手法が異なるほかは略同様の手順にて実現される。

【００３８】本実施の形態によれば、リモートアクセス制御サーバ２２において、ユーザがアクセス可能なサーバ、および、各サーバをアクセスするためのそれぞれの固有パスワード（認証情報）を記憶し、ユーザのアクセスにより、ユーザがアクセス可能なサーバのリストを含むメニュー画像を提示し、メニュー項目の選択にしたがって、選択されたメニュー項目に関するサーバをアクセスするためのユーザ固有のパスワードを利用して、認証を代理して実行する。したがって、ユーザは、サーバのアクセスごとに、ユーザＩＤやパスワードの入力をする必要がなく、イントラネット２４に接続された所望のサーバにアクセスして、所望のコンテンツを取得することが可能となる。

【００３９】本発明は、以上の実施の形態に限定されることなく、特許請求の範囲に記載された発明の範囲内で、種々の変更が可能であり、それらも本発明の範囲内に包含されるものであることは、言うまでもない。たとえば、前記実施の形態においては、携帯端末からのアクセスについて説明したが、これに限定されず、通常のパーソナルコンピュータからのアクセスについても本発明を適用できることは明らかである。

【００４０】また、前記実施の形態においては、社内のイントラネット２４へのアクセスに本発明を適用しているが、これに限定されず、地方公共団体、学校など任意の識別のイントラネットへのアクセスのために適用することが可能であることは言うまでもない。さらに、イントラネット２４に限られず、インターネット１２上であっても、一定のサーバ群が、リモートアクセス制御サーバ２２を介してアクセスできるような構成に適用しても良い。

【００４１】また、本実施の形態においては、リモートアクセス制御サーバ２２が、ベーシック認証、ＩＭＡＰ認証など、代理して実行しているが、リモートアクセス制御サーバ２２が代理して実行できる認証種別は、上述したものに限定されるものではない。なお、本明細書において、一つの手段の機能が、二つ以上の物理的手段により実現されても、若しくは、二つ以上の手段の機能が、一つの物理的手段により実現されてもよい。

【００４２】

【発明の効果】本発明によれば、ユーザによる煩雑な入力なしに、一定のサーバにアクセス可能となるような手法を提供することが可能となる。

【図面の簡単な説明】

【図１】　図１は、本発明の実施の形態にかかるデータ通信システムの概略を示す図である。

【図２】　図２は、本実施の形態にかかるリモートアクセス制御サーバの構成を示すブロックダイヤグラムである。

【図３】　図３は、本実施の形態において、携帯端末、リモートアクセス制御サーバなどにて実行される処理を示すフローチャートである。

【図４】　図４は、本実施の形態にかかるユーザアクセス情報ＤＢ中のデータ構造、および、イントラネットサーバ情報ＤＢのデフォルト情報領域の例を示す図である。

【図５】　図５は、本実施の形態において、携帯端末、リモートアクセス制御サーバなどにて実行される処理を示すフローチャートである。

【図６】　図６は、本実施の形態にかかるイントラネットサーバ情報ＤＢ中、各サーバの情報領域の例を示す図である。

【図７】　図７は、本実施の形態において、携帯端末の表示装置の画面上に表示された画像の例を示す図である。

【符号の説明】

| | |
|---|---|
| １２ | インターネット |
| １４ | 携帯端末 |
| １６ | 制御システム |
| １８ | プロキシサーバ |
| ２０ | ＨＴＭＬ変換サーバ |
| ２２ | リモートアクセス制御サーバ |
| ２４ | イントラネット |
| ２６ | サーバ |
| ３４ | ユーザ認証部 |
| ３６ | ユーザ認証情報ＤＢ |
| ３８ | 初期アクセスメニュー生成部 |
| ４０ | ユーザアクセス情報ＤＢ |
| ４２ | イントラネットサーバ情報ＤＢ |
| ４４ | ＨＴＭＬ整形／表示部 |
| ４６ | アクセス情報受理部 |
| ５０ | 情報取得部 |

【図１】

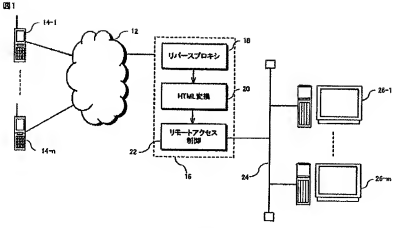


図1
14-1
14-m
12
18
リバースプロキシ
20
HTML変換
リモートアクセス制御
22
16
24
26-1
26-m

【図２】

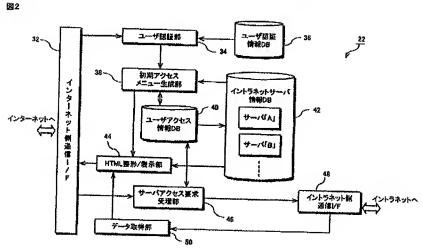


図2
32
ユーザ認証部
ユーザ認証情報DB
36
34
22
38
初期アクセスメニュー生成部
イントラネットサーバ情報DB
インターネットへ
ユーザアクセス情報DB
40
42
サーバA
サーバB
インターネット側通信I/F
44
HTML解析/書換部
サーバアクセス要求受信部
48
イントラネット側通信I/F
イントラネットへ
46
データ取得部
50

【図７】

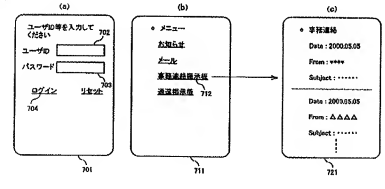


図7
(a)
ユーザID等を入力してください
ユーザID
パスワード
ログイン
リセット
702
703
704
701
(b)
メニュー
お知らせ
メール
車載連絡掲示板
通信履歴照会
712
711
(c)
車載連絡
Date : 2000.05.05
From : ****
Subject : ******
Date : 2000.05.05
From : △△△△
Subject : ******
721

【図３】

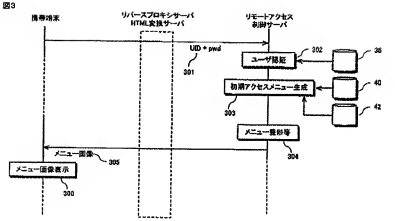


図3
携帯端末
リバースプロキシサーバ
HTML変換サーバ
リモートアクセス
制御サーバ
UID + pwd
301
302
ユーザ認証
36
物理アクセスメニュー生成
40
42
303
メニュー登録等
304
メニュー画像
305
メニュー画像表示
300

【図５】

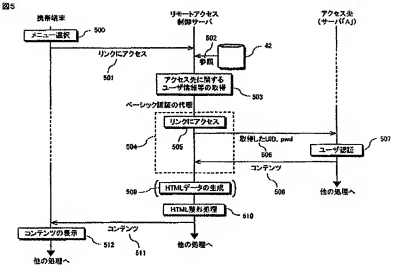
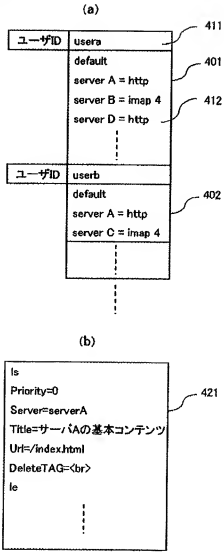


図5
携帯端末
リモートアクセス
制御サーバ
アクセス先
（サーバA）
メニュー選択
500
502
42
事前
リンクにアクセス
501
アクセス先に関する
ユーザ情報等の取得
503
ベーシック認証の代理
リンクにアクセス
504
505
取得したUID, pwd
507
ユーザ認証
506
コンテンツ
HTMLデータの生成
508
509
他の処理へ
HTML整形処理
510
コンテンツの表示
512
コンテンツ
511
他の処理へ
他の処理へ

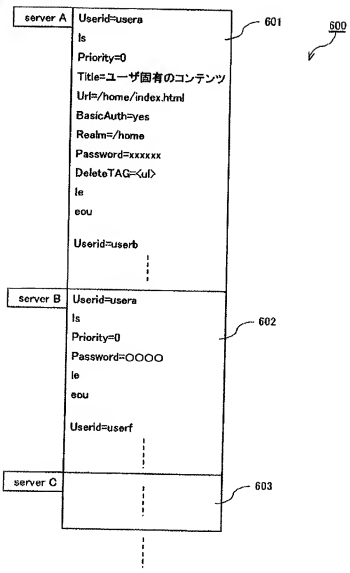
【図４】

図4


(a)
ユーザID
usera
411
default
server A = http
server B = imap 4
server D = http
401
412
ユーザID
userb
default
server A = http
server C = imap 4
402
(b)
ls
Priority=0
Server=serverA
Title=サーバAの基本コンテンツ
Url=/index.html
DeleteTAG=<br>
le
421

【図６】

図6




フロントページの続き

| (51) Int. Cl.[7] | 識別記号 | F I | テーマコード（参考） |
|---|---|---|---|
| G06F 13/00 | 510 | G06F 13/00 | 510A |